Remarks

Applicant respectfully requests reconsideration of this application. The specification has been amended to correct minor informalities. Claims 1-27 and 30 have been canceled. Claims 37-46 are withdrawn. Claims 28-29 and 31-34 have been amended. New claims 47-51 are presented for examination. No claims stand allowed.

Information Disclosure Statement

Applicant wishes to disclose the status of other applications that may be considered related to the present application, as follows: serial no.: 10/315,624 (Office Action rejecting all pending claims mailed 04/09/09); serial no.: 10/367,178 (Final Office Action rejecting all pending claims mailed 12/12/08); serial no.: 10/315,694 (issued as US 7,493,078; 02/19/09); serial no.: 10/367,197 (Final Office Action rejecting all pending claims mailed 12/11/08); serial no.: 10/889,326 (Office Action rejecting all pending claims mailed 02/04/09); serial no.: 10/608,594 (Office Action rejecting all pending claims mailed 02/04/09); serial no.: 10/618,931 (Office Action rejecting all pending claims mailed 02/18/09); serial no.: 10/315,788 (Notice of Allowance mailed 05/15/09); serial no.: 10/395,749 (Office Action rejecting all pending claims mailed 07/16/08); serial no.: 10/407,445 (Office Action rejecting all pending claims mailed 02/05/09); serial no.:11/800,543 (issued as US 7,741,665; 05/05/07); and serial no.: 10/435,005 (issued as US 7,215,660; 05/08/07).

Traversal of Claim Rejections Under 35 U.S.C. § 112, 1st ¶

Claim 28-36 stand rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Applicant respectfully submits that this rejection is rendered moot in view of the amendments to claims 28-29 and 31-34, as well as the cancellation of claim 30. Support for amended claim 28 is

found throughout the specification and drawings. For example, paragraph [0081] specifically describes the claimed operation of network adaptation in conjunction with Figures 17A-17B and 18A-18B. Paragraph [0054] also discloses alternate transmissions (even/odd intervals) on the same frequency channel. Figures 8-13, 14A-14C, along with corresponding portions of the specification also disclose elements and limitations of the subject claims. Paragraphs [0009], [0013], [0058], for example, disclose data throughputs of at least 11Mbps over a WLAN. Similarly, data throughputs of 36Mbps are shown in Figures 10, 12, and 14.

Applicant respectfully submits that the amended claims satisfy the requirements of the statute since the specification and drawings clearly indicate to persons skilled in the art that, as of the filing date, Applicant had invented what is now claimed.

Traversal of Claim Rejections Under 35 U.S.C. § 103(a)

Claims 28-30 and 33-36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Ganz et al. (US 6,584,080; "Ganz") in view of Oura (US 6,115,369; "Oura"); and Ganz in view of Heinonen et al. (US 6,968,153 B1; "Heinonen"). Additionally, claims 31 and 32 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Ganz in view of Heinonen and further in view of Lau et al. (US 6,690,657 "Lau").. Applicant respectfully traverses each of these grounds of rejection.

Ganz teaches a conventional radio communication repeater system in which each repeater is strictly limited to line-of-sight data transmissions with another repeater. (See e.g., column 2, lines 48-55) Stated differently, Ganz fails to disclose or teach data transmissions to a next repeater that is physically obstructed (or becomes physically obstructed after installation) from a line-of-sight view. Because of the physical positioning and path clearing requirements, line-of-sight transmission

systems typically require human intervention for re-configuration and are unable to self-re-configure. Furthermore, line-of-sight transmissions are a special case of wireless transmission that can use focused beams and do not have to address the challenges of channel conflict resolution inherent with non-line-of-sight transmission.

Oura teaches the use of Time Division Multiple Access-Time Division Duplex (TDMA-TDD) technology for a cellular phone network. TDMA is a technology for delivering digital wireless service using time-division multiplexing (TDM). TDMA is a well-known audio communication technique that works by dividing a radio frequency into time slots and then allocating slots to multiple calls. In this way, a single frequency can support multiple, simultaneous data channels. TDMA, for example, is used by the Global Systems for Mobile (GSM) digital cellular telephone system. TDMA technology basically shares a communications channel among several phone calls. TDD is commonly used with TDMA in cellular phone networks to allow a number of different users to receive forward channel signals and then, in turn, transmit reverse channel signals using the same carrier frequency.

Applicant respectfully submits that Oura is non-analogous art since a person of ordinary skill would not reasonably be expected to look to the field of mobile telephone systems for a solution to the problem of wireless transmission of real-time audiovisual content. By way of example, Oura discloses that audio information is transmitted at data speeds of 384 kbps. (Column 4, lines 30-39) In contrast, the claimed subject matter defines a wireless repeater operating at a data throughput of at least 11Mbps. Given the enormous difference in transmission rates and the completely different problems faced when transmitting audiovisual content versus simple voice data, Applicant respectfully submits that a person or skill working in the field of wireless transmission of high-speed (e.g., real-time audiovisual) data would not consider mobile phone communication systems to be within the same field of endeavor as the claimed subject matter.

Even if Oura were considered analogous art, Applicant respectfully submits that a person of ordinary skill would not have been motivated to modify or combine Ganz with Oura to arrive at the claimed invention. One reason why is because the combined teachings of Ganz and Oura fail to teach or suggest a wireless repeater operating at a data throughput of at least 11Mbps. Furthermore, a person of ordinary skill in the wireless networking arts would have understood that the CSMA/CA and TDMA techniques taught by Oura suffer the disadvantage of a throughput limitation of about 1 Mbps, with a range limitation of less than typical household dimension, bandwidth inadequate for multimedia, limitations in the number of active devices, and wasted bandwidth. Indeed, Lau disparages TDM approaches such as Oura's as being inadequate due to these very limitations (see column 2, line 25 through column 3 line 29).

Lau teaches the user of low-power transceivers in channel-shifting RF repeaters to create a wireless network that can extend beyond each transceiver's useful range. A base station controls the allocation of time on one or more available channels between competing transmitters, and may also control the function of the channel-shifting repeaters. When a given transmitter is transmitting, repeaters in range of that transmitter receive the signal, channel-shift the signal, and retransmit it. (Column 4, lines 6-19)

By teaching a system and method that uses repeaters having multiple transceivers that transmit and receive simultaneously on different frequency channels, Lau teaches away from the approach taken by Applicant. A person of skill reading Lau would therefore have been discouraged from attempting the claimed subject matter since Lau explicitly teaches away from Applicant's solution. Such a skilled person would also have lacked any motivation to attempt to combine Lau with Heinonen and Ganz since Lau specifically teaches that TDMA approaches are limited

to a 1Mbps throughput, a rate that is adequate for a mobile phone system, but which is completely inadequate to transmit real-time audiovisual data content.

Applicant therefore respectfully submits that a person of ordinary skill, upon reading the Lau reference, would be discouraged from attempting a method comprising adapting a WLAN to a channel conflict by re-configuring a first repeater in a branch of a repeater topology to re-use a certain channel already in use by a neighboring repeater, the first repeater and the neighboring repeater being physically obstructed from a line-of-sight view, the first repeater being re-configured to transmit data at a data throughput of at least 11Mbps on the certain channel during even time intervals and receive data at the data throughput on the certain channel during odd time intervals, the neighboring repeater transmitting during the odd time intervals and receiving during the even time intervals, as recited, for example, in amended claim 28.

Heinonen likewise fails to teach receiving and transmitting at alternating or staggered time intervals. Heinonen instead teaches a Bluetooth repeater that may receive Bluetooth communications from an originating Bluetooth enabled device within range and then forward the same data to an intended recipient outside the range of the originating Bluetooth enabled device. Although Bluetooth is a radio frequency (RF) technology that operates at 2.4 GHz and is capable of transmitting voice and data, the effective range of Bluetooth devices is very short (e.g., 10 meters) and Bluetooth transfers data at the limited rate of about 1 Mbps, which is far less than what is needed for high-quality, high-bandwidth video transmissions using any known technology today, let alone at the time of Applicant's invention.

A person of ordinary skill in the art would have lacked any motivation to combine / modify Ganz with Heinonen to arrive at the claimed subject matter because both references are limited to very slow data throughputs – at least an order of magnitude less than that defined by the claimed invention. Simply put, a person of ordinary skill in the art would have lacked any reasonable expectation of success in

attempting any such combination due to the throughput limitations of the prior art references.

The same is true with respect to the combined teachings of Lau, Ganz and Heinonen. Lau teaches away from transmission techniques like Bluetooth that have limited data throughput. Lau also teaches away from technologies that have transmission range limitations, which Ganz and Heinonen certainly suffer from. Given Lau's disparaging remarks about technologies such as Bluetooth, Applicant respectfully submits that a person of ordinary skill in the art would have lacked any motivation to combine / modify Lau with Heinonen and/or Ganz to arrive at the claimed subject matter. Furthermore, Applicant respectfully submits that such an ordinary practitioner would certainly have lacked any reasonable expectation of success at achieving the claimed invention in of any such combination. One reason why is because both Ganz and Heinonen lacks any enabling teaching of a system capable of delivering high-quality, high-bandwidth video transmissions video transmission over a system that utilizes non-line-of-sight repeaters to extend transmissions.

Heinonen is limited to teaching Bluetooth repeaters in combination with Bluetooth source and destination devices. In this regard, the shortcomings of Bluetooth technology are well known to persons of ordinary skill in the art. Heinonen does not teach the use of 802.11a, b, or g transceivers with data throughputs that exceed 30 Mbps. The only reference to 802.11 technologies in Heinonen is found in a single sentence of column 4, lines 10-15, which reads, preceded by two contextual sentences:

> "Each pair is comprised of two Bluetooth chips C1 and C2. In one embodiment, the repeater pairs 193, 193b block out all communications other than transmissions coming from the other pair. In an alternative embodiment, a portion of each repeater pair is replaced with another communications link such as, but not limited to: Bluetooth with directed

antenna; cellular; IEEE 802.11a, b and g; physical links (i.e., Ethernet, twisted pair wiring, CAT 5 cabling, etc.); and/or the like.

Applicant respectfully submits that such a configuration would limit the transmitted data rate to the data rate of the slowest link in any repeater pair. Since each repeater pair explicitly includes at least one Bluetooth chip C1 or C2, the data rate of any configuration is limited to the 1Mbps data rate of Bluetooth. This teaches away from any configuration that would support high data rate transmissions (e.g., 11Mbps) over a wireless network that includes a plurality of repeaters arranged in a transmission chain. Furthermore, this single sentence of Heinonen provides no clue to a person of ordinary skill how to combine Bluetooth devices (which are limited to transfer rates of about 1 Mbps) with an IEEE 802.11a, b, or g communications link in such a way as to be able to arrive at data throughputs at least 10 times greater than the limited capabilities of Bluetooth.

Applicant wishes to point out that the embodiment of Figure 3 of Heinonen is limited, in its entirety, to Bluetooth devices (D1-D4), such that the system shown in Figure 3 has a maximum data transfer rate of about 1 Mbps, which is at least an order of magnitude slower than that specified in the subject claims, and a speed that makes it totally unfeasible to transmit high-quality video. To aid in the Examiner's understanding, the Wikipedia article entitled, "Bluetooth" (http://en.wikipedia.org/wiki/Bluetooth) is attached as extrinsic evidence of the common meaning of Bluetooth technology to a person of skill in the communication arts. This article also explains the very limitations which make Bluetooth not only unattractive, but unfeasible for high data rate video applications.

It should be understood that Heinonen also fails to teach any protocol or scheme for avoiding frequency interference so as to not compromise data throughput through the network. Rather, Heinonen's purpose is to extend the range of Bluetooth devices by use of standard Bluetooth repeaters, without any concern to the impact

this extension of range would have on data throughput. Given that Bluetooth was designed for low-bandwidth devices (e.g., input peripherals and audio devices) this is a reasonable trade-off since maximizing throughput is rarely a concern for Bluetooth applications. But Heinonen's approach would necessarily defeat the data throughput rate of a wireless repeater network attempting to approach the maximum throughput that is available in the wireless spectrum. In other words, Heinonen fails to teach transmitting and re-transmitting packets at a data throughput of at least 11Mbps or greater in a wireless network that includes a plurality of repeaters.

In sum, neither Oura nor Heinonen nor Lau provide any of the teaching missing from the base Ganz reference. Moreover, given that Lau explicitly disparages approaches such as those taught by Ganz, Oura and Heinonen, Applicant respectfully submits that a person of ordinary skill in the art would have lacked any reason to combine or modify these references in the manner suggested by the Examiner. Furthermore, such an ordinary practitioner would have had no reasonable expectation of success at achieving Applicant's claimed invention in view of the Examiner's selective combination of the teachings of the cited references.

Applicant respectfully submits that for all the reasons given above that a person of ordinary skill in the art considering the cited prior art references at the time of Applicant's invention would have not been led to, or able to achieve, the subject matter of Applicant's amended claims.

Accordingly, Applicant respectfully requests that the rejections under 35 U.S.C. § 103(a) be withdrawn. Applicant respectfully submits that all remaining claims are now in condition for allowance.

Please charge any shortages of fees or credit any overcharges of fees to our Deposit Account No. 50-2060.

Respectfully submitted,
THE LAW OFFICES OF BRADLEY J. BEREZNAK

Dated: 7/6, 2009

Bradley J. Bereznak
Attorney for Applicant
Registration No. 33,474

800 West El Camino Real
Suite 180
Mt. View, CA 94040
(650) 903-2264

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to: Mail Stop RCE Amendments, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on July 6, 2009.

Anna Iosifova — July 6, 2009 (Date)

Bluetooth

From Wikipedia, the free encyclopedia

Bluetooth is an open wireless protocol for exchanging data over short distances from fixed and mobile devices, creating personal area networks (PANs). It was originally conceived as a wireless alternative to RS232 data cables. It can connect several devices, overcoming problems of synchronization.

Bluetooth logo.

Contents

Name and logo

The word *Bluetooth* is an anglicized version of Old Norse *Blátönn* or Danish *Blåtand*, the name of the tenth-century king Harald I of Denmark, who united dissonant Danish tribes into a single kingdom. The implication is that Bluetooth does the same with communications protocols, uniting them into one universal standard.[1][2][3]

The Bluetooth logo is a bind rune merging the Germanic runes ᚼ (Hagall) and ᛒ (Berkanan).

Implementation

Bluetooth uses a radio technology called frequency-hopping spread spectrum, which chops up the data being sent and transmits chunks of it on up to 79 frequencies. In its basic mode, the modulation is Gaussian frequency-shift keying (GFSK). It can achieve a gross data rate of 1 Mb/s. Bluetooth provides a way to connect and exchange information between devices such as mobile phones, telephones, laptops, personal computers, printers, Global Positioning System (GPS) receivers, digital cameras, and video game consoles through a secure, globally unlicensed Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency bandwidth. The Bluetooth specifications are developed and licensed by the Bluetooth Special Interest Group (SIG). The Bluetooth SIG consists of companies in the areas of telecommunication, computing, networking, and consumer electronics.[4]

Uses

Bluetooth is a standard and communications protocol primarily designed for low power consumption, with a short range (power-class-dependent: 1 meter, 10 meters, 100 meters) based on low-cost transceiver microchips in each device.[5] Bluetooth makes it possible for these devices to communicate with each other when they are in range. Because the devices use a radio (broadcast) communications system, they do not have to be in line of sight of each other.[4]

Class	Maximum Permitted Power mW (dBm)	Range (approximate)
Class 1	100 mW (20 dBm)	~100 meters
Class 2	2.5 mW (4 dBm)	~10 meters
Class 3	1 mW (0 dBm)	~1 meter

In most cases the effective range of class 2 devices is extended if they connect to a class 1 transceiver, compared to a pure class 2 network. This is accomplished by the higher sensitivity and transmission power of Class 1 devices.

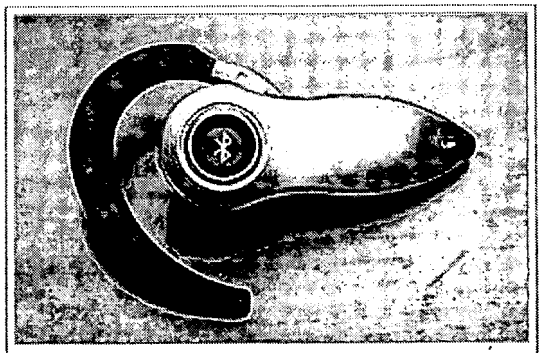
Version	Data Rate
Version 1.2	1 Mbit/s
Version 2.0 + EDR	3 Mbit/s

Bluetooth profiles

In order to use Bluetooth, a device must be compatible with certain Bluetooth profiles. These define the possible applications and uses of the technology.

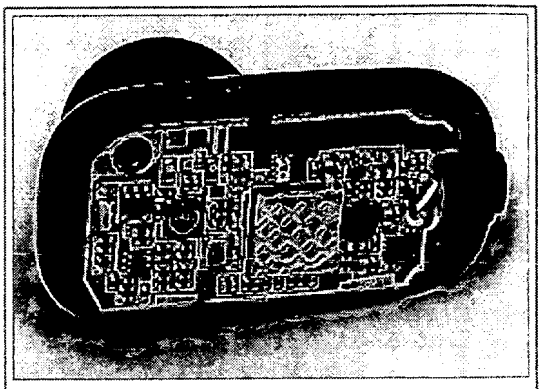
List of applications

More prevalent applications of Bluetooth include:


A typical Bluetooth mobile phone headset.

- Wireless control of and communication between a mobile phone and a hands-free headset. This was one of the earliest applications to become popular.
- Wireless networking between PCs in a confined space and where little bandwidth is required.
- Wireless communication with PC input and output devices, the most common being the mouse, keyboard and printer.
- Transfer of files, contact details, calendar appointments, and reminders between devices with OBEX.
- Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.
- For controls where infrared was traditionally used.
- For low bandwidth applications where higher [USB] bandwidth is not required and cable-free connection desired.

- Sending small advertisements from Bluetooth-enabled advertising hoardings to other, discoverable, Bluetooth devices.
- Wireless bridge between two Industrial Ethernet (e.g. PROFINET) networks.
- Two seventh-generation game consoles, Nintendo's Wii[6] and Sony's PlayStation 3, use Bluetooth for their respective wireless controllers.
- Dial-up internet access on personal computers or PDAs using a data-capable mobile phone as a modem.



Nokia BH-208 headset internals.

Bluetooth IEEE 802.15.1 vs. Wi-Fi IEEE 802.11 in networking

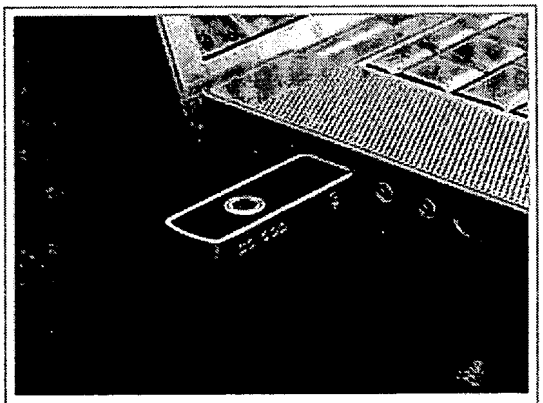
Bluetooth and Wi-Fi have many applications in today's offices, homes, and on the move: setting up networks, printing, or transferring presentations and files from PDAs to computers. Both are versions of unlicensed wireless technology.

Wi-Fi is intended for resident equipment and its applications. The category of applications is outlined as WLAN, the wireless local area networks. Wi-Fi is intended as a replacement for cabling for general local area network access in work areas.

Bluetooth is intended for non resident equipment and its applications. The category of applications is outlined as the wireless personal area network (WPAN). Bluetooth is a replacement for cabling in a variety of personally carried applications in any ambience.

Bluetooth devices

Bluetooth exists in many products, such as telephones, the Wii, PlayStation 3, Lego Mindstorms NXT and recently in some high definition watches, modems and headsets. The technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations. Bluetooth is commonly used to transfer sound data with telephones (i.e., with a Bluetooth headset) or byte data with hand-held computers (transferring files).



A Bluetooth USB dongle with a 100 m range.

Bluetooth protocols simplify the discovery and setup of services between devices. Bluetooth devices can advertise all of the services they provide. This makes using services easier because more of the security, network address and permission configuration can be automated than with many other network types.

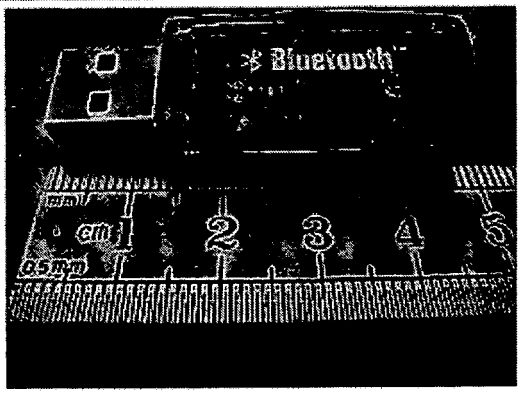
Wi-Fi

Wi-Fi is a traditional Ethernet network, and requires configuration to set up shared resources, transmit files, and to set up audio links (for example, headsets and hands-free devices). Wi-Fi uses the same radio frequencies as Bluetooth, but with higher power, resulting in a stronger connection. Wi-Fi is sometimes

called "wireless Ethernet." This description is accurate, as it also provides an indication of its relative strengths and weaknesses. Wi-Fi requires more setup but is better suited for operating full-scale networks; it enables a faster connection, better range from the base station, and better security than Bluetooth.

Computer requirements

A personal computer must have a Bluetooth adapter in order to communicate with other Bluetooth devices (such as mobile phones, mice and keyboards). While some desktop computers and most recent laptops come with a built-in Bluetooth adapter, others will require an external one in the form of a dongle.



A typical Bluetooth USB dongle.

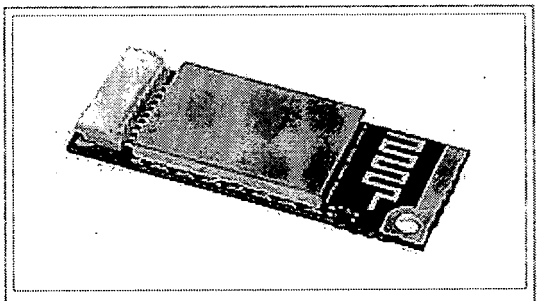
Unlike its predecessor, IrDA, which requires a separate adapter for each device, Bluetooth allows multiple devices to communicate with a computer over a single adapter.

Operating system support

For more details on this topic, see Bluetooth stack.

Apple has supported Bluetooth since Mac OS X v10.2 which was released in 2002.[7]

For Microsoft platforms, Windows XP Service Pack 2 and later releases have native support for Bluetooth. Previous versions required users to install their Bluetooth adapter's own drivers, which were not directly supported by Microsoft.[8] Microsoft's own Bluetooth dongles (packaged with their Bluetooth computer devices) have no external drivers and thus require at least Windows XP Service Pack 2.


An internal notebook Bluetooth card (14×36×4 mm).

Linux has two popular Bluetooth stacks, BlueZ and Affix. The BlueZ[9] stack is included with most Linux kernels and was originally developed by Qualcomm. The Affix stack was developed by Nokia. FreeBSD features Bluetooth support since its 5.0 release. NetBSD features Bluetooth support since its 4.0 release. Its Bluetooth stack has been ported to OpenBSD as well.

Mobile phone requirements

A mobile phone that is Bluetooth enabled is able to pair with many devices. To ensure the broadest support of feature functionality together with legacy device support, the Open Mobile Terminal Platform (OMTP) forum has recently published a recommendations paper, entitled "Bluetooth Local Connectivity"; see external links below to download this paper.

Specifications and features

The Bluetooth specification was developed in 1994 by Jaap Haartsen and Sven Mattisson, who were working for Ericsson Mobile Platforms in Lund, Sweden.[10] The specification is based on frequency-hopping spread spectrum technology.

The specifications were formalized by the Bluetooth Special Interest Group (SIG). The SIG was formally announced on May 20, 1998. Today it has a membership of over 11,000 companies worldwide. It was established by Ericsson, IBM, Intel, Toshiba, and Nokia, and later joined by many other companies.

Bluetooth 1.0 and 1.0B

Versions 1.0 and 1.0B had many problems, and manufacturers had difficulty making their products interoperable. Versions 1.0 and 1.0B also included mandatory Bluetooth hardware device address (BD_ADDR) transmission in the Connecting process (rendering anonymity impossible at the protocol level), which was a major setback for certain services planned for use in Bluetooth environments.

Bluetooth 1.1

- Ratified as IEEE Standard 802.15.1-2002.
- Many errors found in the 1.0B specifications were fixed.
- Added support for non-encrypted channels.
- Received Signal Strength Indicator (RSSI).

Bluetooth 1.2

This version is backward compatible with 1.1 and the major enhancements include the following:

- Faster Connection and Discovery
- *Adaptive frequency-hopping spread spectrum (AFH)*, which improves resistance to radio frequency interference by avoiding the use of crowded frequencies in the hopping sequence.
- Higher transmission speeds in practice, up to 721 kbit/s, than in 1.1.
- Extended Synchronous Connections (eSCO), which improve voice quality of audio links by allowing retransmissions of corrupted packets, and may optionally increase audio latency to provide better support for concurrent data transfer.
- Host Controller Interface (HCI) support for three-wire UART.
- Ratified as IEEE Standard 802.15.1-2005.
- Introduced Flow Control and Retransmission Modes for L2CAP.

Bluetooth 2.0

This version of the Bluetooth specification was released on November 10, 2004. It is backward compatible with the previous version 1.2. The main difference is the introduction of an Enhanced Data Rate (EDR) for faster data transfer. The nominal rate of EDR is about 3 megabits per second, although the practical data transfer rate is 2.1 megabits per second.[11] The additional throughput is obtained by using a different radio technology for transmission of the data. Standard, or Basic Rate, transmission uses Gaussian Frequency Shift Keying (GFSK) modulation of the radio signal with a gross air data rate

of 1 Mbit/s. EDR uses a combination of GFSK and Phase Shift Keying modulation (PSK) with two variants, π/4-DQPSK and 8DPSK. These have gross air data rates of 2, and 3 Mbit/s respectively. [12]

According to the 2.0 specification, EDR provides the following benefits:

- Three times the transmission speed — up to 10 times (2.1 Mbit/s) in some cases.
- Reduced complexity of multiple simultaneous connections due to additional bandwidth.
- Lower power consumption through a reduced duty cycle.

The Bluetooth Special Interest Group (SIG) published the specification as "Bluetooth 2.0 + EDR" which implies that EDR is an optional feature. Aside from EDR, there are other minor improvements to the 2.0 specification, and products may claim compliance to "Bluetooth 2.0" without supporting the higher data rate. At least one commercial device, the HTC TyTN Pocket PC phone, states "Bluetooth 2.0 without EDR" on its data sheet.[13]

Bluetooth 2.1

Bluetooth Core Specification Version 2.1 is fully backward compatible with 1.2, and was adopted by the Bluetooth SIG on July 26, 2007.[12] This specification includes the following features:

- **Extended Inquiry Response** (EIR): provides more information during the inquiry procedure to allow better filtering of devices before connection. This information may include the name of the device, a list of services the device supports, the transmission power level used for inquiry responses, and manufacturer defined data.

- **Sniff Subrating**: reduces the power consumption when devices are in the sniff low-power mode, especially on links with asymmetric data flows. Human interface devices (HID) are expected to benefit the most, with mouse and keyboard devices increasing their battery life by a factor of 3 to 10. It lets devices decide how long they will wait before sending keepalive messages to one another. Previous Bluetooth implementations featured keep alive message frequencies of up to several times per second. In contrast, the 2.1 specification allows pairs of devices to negotiate this value between them to as infrequently as once every 5 or 10 seconds.

- **Encryption Pause Resume** (EPR): enables an encryption key to be changed with less management required by the Bluetooth host. Changing an encryption key must be done for a role switch of an encrypted an ACL link, or every 23.3 hours (one Bluetooth day) encryption is enabled on an ACL link. Before this feature was introduced, when an encryption key is refreshed the Bluetooth host would be notified of a brief gap in encryption while the new key was generated; so the Bluetooth host was required to handle pausing data transfer (however data requiring encryption may already have been sent before the notification that encryption is disabled has been received). With EPR, the Bluetooth host is not notified of the gap, and the Bluetooth controller ensures that no unencrypted data is transferred while they key is refreshed.

- **Secure Simple Pairing** (SSP): radically improves the pairing experience for Bluetooth devices, while increasing the use and strength of security. It is expected that this feature will significantly increase the use of Bluetooth.[14]

- Near Field Communication (NFC) cooperation: automatic creation of secure Bluetooth connections when NFC radio interface is also available. This functionality is part of the Secure Simple Pairing where NFC is one way of exchanging pairing information. For example, a headset should be paired with a Bluetooth 2.1 phone including NFC just by bringing the two devices close

to each other (a few centimeters). Another example is automatic uploading of photos from a mobile phone or camera to a digital picture frame just by bringing the phone or camera close to the frame.[15][16]

Bluetooth 3.0

The 3.0 specification[12] was adopted by the Bluetooth SIG (https://www.bluetooth.org/apps/content/) on April 21st, 2009. Its main new feature is AMP (Alternate MAC/PHY), the addition of 802.11 as a high speed transport. Two technologies had been anticipated for AMP: 802.11 and UWB, but UWB is missing from the specification[17].

- **Alternate MAC PHY**: enables the use of alternative MAC and PHY's for transporting Bluetooth profile data. The Bluetooth Radio is still used for device discovery, initial connection and profile configuration, however when lots of data needs to be sent, the high speed alternate MAC PHY (802.11, typically associated with Wi-Fi) will be used to transport the data. This means that the proven low power connection models of Bluetooth are used when the system is idle, and the low power per bit radios are used when lots of data needs to be sent.
- **Unicast Connectionless Data**: permits service data to be sent without establishing an explicit L2CAP channel. It is intended for use by applications that require low latency between user action and reconnection/transmission of data. This is only appropriate for small amounts of data.
- **Read Encryption Key Size**: introduces a standard HCI command for a Bluetooth host to query the encryption key size on an encrypted ACL link. The encryption key size used on a link is required for the SIM Access Profile, so generally Bluetooth controllers provided this feature in a proprietary manner. Now the information is available over the standard HCI interface.

Bluetooth low energy

On April 20, 2009, Bluetooth SIG presented the new Bluetooth low energy as an entirely additional protocol stack, compatible with other existing Bluetooth protocol stacks. The preceding naming as 'Wibree' and 'Bluetooth ULP' (Ultra Low Power) has been outdated by the final naming as 'Bluetooth low energy'.

On June 12, 2007, Nokia and Bluetooth SIG had announced that Wibree will be a part of the Bluetooth specification, as an ultra-low power Bluetooth technology.[18] Expected use cases include watches displaying Caller ID information, sports sensors monitoring the wearer's heart rate during exercise, and medical devices. The Medical Devices Working Group is also creating a medical devices profile and associated protocols to enable this market. Bluetooth low energy technology is designed for devices to have a battery life of up to one year.

Future

- **Broadcast Channel**: enables Bluetooth information points. This will drive the adoption of Bluetooth into mobile phones, and enable advertising models based around users pulling information from the information points, and not based around the object push model that is used in a limited way today.

- **Topology Management**: enables the automatic configuration of the piconet topologies especially in scatternet situations that are becoming more common today. This should all be invisible to the users of the technology, while also making the technology just work.

- QoS improvements: enable audio and video data to be transmitted at a higher quality, especially when best effort traffic is being transmitted in the same piconet.

UWB for AMP

The high speed (AMP) feature of Bluetooth 3.0 is based on 802.11, but the AMP mechanism was designed to be usable with other radios as well. It was originally intended for UWB, but the WiMedia Alliance, the body responsible for the flavor of UWB intended for Bluetooth, announced in March 2009 that it was disbanding.

On March 16, 2009, the WiMedia Alliance announced it was entering into technology transfer agreements for the WiMedia Ultra-wideband (UWB) specifications. WiMedia will transfer all current and future specifications, including work on future high speed and power optimized implementations, to the Bluetooth Special Interest Group (SIG), Wireless USB Promoter Group and the USB Implementers Forum. After the successful completion of the technology transfer, marketing and related administrative items, the WiMedia Alliance will cease operations.[19]

Technical information

Bluetooth protocol stack

"Bluetooth is defined as a layer protocol architecture consisting of core protocols, cable replacement protocols, telephony control protocols, and adopted protocols".[20]

Mandatory protocols for all Bluetooth stacks are: LMP, L2CAP and SDP

Additionally, these protocols are almost universally supported: HCI and RFCOMM

LMP (Link Management Protocol)

Used for control of the radio link between two devices. Implemented on the controller.

L2CAP (Logical Link Control & Adaptation Protocol)

Used to multiplex multiple logical connections between two devices using different higher level protocols. Provides segmentation and reassembly of on-air packets.

In Basic mode, L2CAP provides packets with a payload configurable up to 64kB, with 672 bytes as the default MTU, and 48 bytes as the minimum mandatory supported MTU.

In Retransmission & Flow Control modes, L2CAP can be configured for reliable or isochronous data per channel by performing retransmissions and CRC checks.

Bluetooth Core Specification Addendum 1 adds two additional L2CAP modes to the core specification. These modes effectively deprecate original Retransmission and Flow Control modes:

- **Enhanced Retransmission Mode** (ERTM): This mode is an improved version of the original retransmission mode. This mode provides a reliable L2CAP channel.

- **Streaming Mode** (SM): This is a very simple mode, with no retransmission or flow control. This mode provides an unreliable L2CAP channel.

Reliability in any of these modes is optionally and/or additionally guaranteed by the lower layer Bluetooth BDR/EDR air interface by configuring the number of retransmissions and flush timeout (time after which the radio will flush packets). In-order sequencing is guaranteed by the lower layer.

Only L2CAP channels configured in ERTM or SM may be operated over AMP logical links.

SDP (Service Discovery Protocol)

Used to allow devices to discover what services each other support, and what parameters to use to connect to them. For example, when connecting a mobile phone to a Bluetooth headset, SDP will be used to determine which Bluetooth profiles are supported by the headset (Headset Profile, Hands Free Profile, Advanced Audio Distribution Profile etc) and the protocol multiplexer settings needed to connect to each of them. Each service is identified by a Universally Unique Identifier (UUID), with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128)

HCI (Host/Controller Interface)

Standardised communication between the host stack (e.g. a PC or mobile phone OS) and the controller (the Bluetooth I.C.) This standard allows the host stack or controller I.C. to be swapped with minimal adaptation.

There are several HCI transport layer standards, each using a different hardware interface to transfer the same command, event and data packets. The most commonly used are USB (in PCs) and UART (in mobile phones and PDAs).

In Bluetooth devices with simple functionality, e.g. headsets, the host stack and controller can be implemented on the same microprocessor. In this case the HCI is optional, although often implemented as an internal software interface.

RFCOMM (Cable replacement protocol)

Radio frequency communications (RFCOMM) is the cable replacement protocol used to create a virtual serial data stream. RFCOMM provides for binary data transport and emulates EIA-232 (formerly RS-232) control signals over the Bluetooth baseband layer.

RFCOMM provides a simple reliable data stream to the user, similar to TCP. It is used directly by many telephony related profiles as a carrier for AT commands, as well as being a transport layer for OBEX over Bluetooth.

Many Bluetooth applications use RFCOMM because of its widespread support and publicly available API on most operating systems. Additionally, applications that used a serial port to communicate can be quickly ported to use RFCOMM.

BNEP (Bluetooth Network Encapsulation Protocol)

BNEP is used to transfer another protocol stack's data via an L2CAP channel. Its main purpose is the transmission of IP packets in the Personal Area Networking Profile. BNEP performs a similar function to SNAP in Wireless LAN.

AVCTP (Audio/Visual Control Transport Protocol)

Used by the remote control profile to transfer AV/C commands over an L2CAP channel. The music control buttons on a stereo headset use this protocol to control the music player

AVDTP (Audio/Visual Data Transport Protocol)

Used by the advanced audio distribution profile to stream music to stereo headsets over an L2CAP channel. Intended to be used by video distribution profile.

Telephone control protocol

Telephony control protocol-binary (TCS BIN) is the bit-oriented protocol that defines the call control signaling for the establishment of voice and data calls between Bluetooth devices. Additionally, "TCS BIN defines mobility management procedures for handling groups of Bluetooth TCS devices"

TCS-BIN is only used by the cordless telephony profile, which failed to attract implementers. As such it is only of historical interest.

Adopted protocols

Adopted protocols are defined by other standards-making organizations and incorporated into Bluetooth's protocol stack, allowing Bluetooth to create protocols only when necessary. The adopted protocols include:

Point-to-Point Protocol (PPP) – Internet standard protocol for transporting IP datagrams over a point-to-point link

TCP/IP/UDP – Foundation Protocols for TCP/IP protocol suite

Object Exchange Protocol (OBEX) – Session-layer protocol for the exchange of objects, providing a model for object and operation representation

Wireless Application Environment / Wireless Application Protocol (WAE/WAP) – WAE specifies an application framework for wireless devices and WAP is an open standard to provide mobile users access to telephony and information services.[20]

Communication and connection

A master Bluetooth device can communicate with up to seven devices in a Wireless User Group. This network group of up to eight devices is called a piconet.

A piconet is an ad-hoc computer network, using Bluetooth technology protocols to allow one master device to interconnect with up to seven active devices. Up to 255 further devices can be inactive, or parked, which the master device can bring into active status at any time.

At any given time, data can be transferred between the master and one other device, however, the devices can switch roles and the slave can become the master at any time. The master switches rapidly from one device to another in a round-robin fashion. (Simultaneous transmission from the master to multiple other devices is possible, but not used much.)

The Bluetooth specification allows connecting two or more piconets together to form a scatternet, with some devices acting as a bridge by simultaneously playing the master role in one piconet and the slave role in another.

Many USB Bluetooth adapters are available, some of which also include an IrDA adapter. Older (pre-2003) Bluetooth adapters, however, have limited services, offering only the Bluetooth Enumerator and a less-powerful Bluetooth Radio incarnation. Such devices can link computers with Bluetooth, but they do not offer much in the way of services that modern adapters do.

Baseband Error Correction

Three types of error correction are implemented in Bluetooth systems,

- 1/3 rate (Forward Error Correction) (FEC)
- 2/3 rate FEC
- Automatic Repeat Request (ARQ)

Setting up connections

Any Bluetooth device will transmit the following information on demand:

- Device name.
- Device class.
- List of services.
- Technical information, for example, device features, manufacturer, Bluetooth specification used, clock offset.

Any device may perform an inquiry to find other devices to connect to, and any device can be configured to respond to such inquiries. However, if the device trying to connect knows the address of the device, it always responds to direct connection requests and transmits the information shown in the list above if requested. Use of a device's services may require pairing or acceptance by its owner, but the connection itself can be initiated by any device and held until it goes out of range. Some devices can be connected to only one device at a time, and connecting to them prevents them from connecting to other devices and appearing in inquiries until they disconnect from the other device.

Every device has a unique 48-bit address. However these addresses are generally not shown in inquiries. Instead, friendly Bluetooth names are used, which can be set by the user. This name appears when another user scans for devices and in lists of paired devices.

Most phones have the Bluetooth name set to the manufacturer and model of the phone by default. Most phones and laptops show only the Bluetooth names and special programs are required to get additional

information about remote devices. This can be confusing as, for example, there could be several phones in range named T610 (see Bluejacking).

Pairing

Pairs of devices may establish a relationship by creating a shared secret known as a *link key*, this process is known as *pairing*. If a link key is stored by both devices they are said to be *bonded*. A device that wants to communicate only with a bonded device can cryptographically authenticate the identity of the other device, and so be sure that it is the same device it previously paired with. Once a link key has been generated, an authenticated ACL link between the devices may be encrypted so that the data that they exchange over the airwaves is protected against eavesdropping. Link keys can be deleted at any time by either device, if done by either device this will implicitly remove the bonding between the devices; so it is possible one of the device to have a link key stored but not be aware that it is no longer bonded to the device associated with the given link key.

Bluetooth services generally require either encryption or authentication, as such require pairing before they allow a remote device to use the given service. Some services, such as the Object Push Profile, elect not to explicitly require authentication or encryption so that pairing does not interfere with the user experience associated with the service use-cases.

Pairing mechanisms have changed significantly with the introduction of Secure Simple Pairing in Bluetooth 2.1. The following summarizes the pairing mechanisms:

- **Legacy pairing**: This is the only method available before Bluetooth 2.1. Each device must enter a PIN code, pairing is only successful if both devices enter the same PIN code. Any 16-digit ACSII string may be used as a PIN code, however not all devices may be capable of entering all possible PIN codes.
  - **Limited Input Devices**: The obvious example of this class of device is a Bluetooth Hands-free headset, which generally have few inputs. These devices usually have a *fixed PIN*, for example "0000" or "1234", that are hard-coded into the device.
  - **Numeric Input Devices**: Mobile phones are classic examples of these devices. They allow a user to enter a numeric value up-to 16 digits in length.
  - **Alpha-numeric Input Devices**: PCs and smartphones are examples of these devices. They allow a user to enter full ASCII text as a PIN code. If pairing with a less capable device the user needs to be aware of the input limitations on the other device, there is no mechanism available for a capable device to determine how it should limit the available input a user may use.
- **Secure Simple Pairing**: This is required by Bluetooth 2.1. A Bluetooth 2.1 device may only use legacy pairing to interoperable with a 2.0 or older device. Secure Simple Pairing uses a type of public key cryptography, and has the following modes of operation:
  - **Just Works**: As implied by the name, this method just works. No user interaction is required; however, a device may prompt the user to confirm the pairing process. This method is typically used by headsets with very limited IO capabilities, and is more secure than the fixed PIN mechanism which is typical for this set of limited devices. This method provides no man in the middle (MITM) protection.
  - **Numeric Comparison**: If both devices have a display and at least one can accept a binary Yes/No user input, they may use Numeric Comparison. This method displays a 6-digit numeric code on each device. The user should compare the numbers to insure they are identical. If the comparison succeeds, the user(s) should confirm pairing on the device(s) that can accept an input. This method provides MITM protection, assuming the user confirms on both devices and actually performs the comparison properly.

- **Passkey Entry**: This method may be used between a device with a display and a device with numeric keypad entry (such as a keyboard), or two devices with numeric keypad entry. In the first case, the display is used to show a 6-digit numeric code to the user, who then enters the code on the keypad. In the second case, the user of each device enters the same 6-digit number. Both cases provide MITM protection.
- **Out of Band** (OOB): This method uses an external means of communication (such as NFC) to exchange some information used in the pairing process. Pairing is completed using the Bluetooth radio, but requires information from the OOB mechanism. This method provides some level of MITM protection, assuming the OOB method used provides MITM.

SSP is considered simple for the following reasons:

- In most cases it does not require a user to generate a passkey.
- For use-cases not requiring MITM, user interaction has been eliminated.
- For Numeric Comparison, MITM protection can be achieved with a simple Yes/No decision by the user.
- Using OOB with NFC will enable pairing when devices simply get close, rather than requiring a lengthy discovery process.

Security Concerns

Prior to Bluetooth 2.1, encryption is not required and can be turned off at any time. Moreover, the encryption key is only good for approximately 23.5 hours; using a single encryption key longer than this time allows simple XOR attacks to retrieve the encryption key.

- Turning off encryption is required for several normal operations, so it is problematic to detect if encryption is disabled for a valid reason or for a security attack.
- Bluetooth 2.1 addresses this in the following ways:
  - Encryption is required for all non SDP (Service Discovery Protocol) connections
  - A new Encryption Pause and Resume feature is used for all normal operations requiring encryption to be disabled. This enables easy identification of normal operation from security attacks.
  - The encryption key is required to be refreshed before it expires.

Link keys may be stored on the device file system, not on the Bluetooth chip itself. Many Bluetooth chip manufacturers allow link keys to be stored on the device; however, if the device is removable this means that the link key will move with the device.

Air interface

The protocol operates in the license-free ISM band at 2.4-2.4835 GHz. To avoid interfering with other protocols that use the 2.45 GHz band, the Bluetooth protocol divides the band into 79 channels (each 1 MHz wide) and changes channels up to 1600 times per second. Implementations with versions 1.1 and 1.2 reach speeds of 723.1 kbit/s. Version 2.0 implementations feature Bluetooth Enhanced Data Rate (EDR) and reach 2.1 Mbit/s. Technically, version 2.0 devices have a higher power consumption, but the three times faster rate reduces the transmission times, effectively reducing power consumption to half that of 1.x devices (assuming equal traffic load).

Security

Overview

Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher. In Bluetooth, key generation is generally based on a Bluetooth PIN, which must be entered into both devices. This procedure might be modified if one of the devices has a fixed PIN, e.g. for headsets or similar devices with a restricted user interface. During pairing, an initialization key or master key is generated, using the E22 algorithm.[21] The E0 stream cipher is used for encrypting packets, granting confidentiality and is based on a shared cryptographic secret, namely a previously generated link key or master key. Those keys, used for subsequent encryption of data sent via the air interface, rely on the Bluetooth PIN, which has been entered into one or both devices.

An overview of Bluetooth vulnerabilities exploits has been published by Andreas Becker.[22]

In September 2008, the National Institute of Standards and Technology (NIST) published a Guide to Bluetooth Security that will serve as reference to organization on the security capabilities of Bluetooth and steps for securing Bluetooth technologies effectively. While Bluetooth has its benefits, it is susceptible to denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. Users/organizations must evaluate their acceptable level of risk and incorporate security into the lifecycle of Bluetooth devices. To help mitigate risks, included in the NIST document are security checklists with guidelines and recommendations for creating and maintaining secure Bluetooth piconets, headsets, and smart card readers.[23]

Bluejacking

Bluejacking is the sending of either a picture or a message from one user to an unsuspecting user through Bluetooth wireless technology. Common applications include short messages (e.g., "You've just been bluejacked!"). [24] Bluejacking does not involve the removal or alteration of any data from the device.

History of security concerns

2001

In 2001, Jakobsson and Wetzel from Bell Laboratories discovered flaws in the pairing protocol of Bluetooth, and also pointed to vulnerabilities in the encryption scheme. [25]

2003

In November 2003, Ben and Adam Laurie from A.L. Digital Ltd. discovered that serious flaws in Bluetooth security may lead to disclosure of personal data.[26] It should be noted, however, that the reported security problems concerned some poor implementations of Bluetooth, rather than the protocol itself.

In a subsequent experiment, Martin Herfurt from the trifinite.group was able to do a field-trial at the CeBIT fairgrounds, showing the importance of the problem to the world. A new attack called BlueBug was used for this experiment.[27] This is one of a number of concerns that have been raised over the security of Bluetooth communications.

2004

In 2004 the first purported virus using Bluetooth to spread itself among mobile phones appeared on the Symbian OS.[28] The virus was first described by Kaspersky Lab and requires users to confirm the installation of unknown software before it can propagate. The virus was written as a proof-of-concept by a group of virus writers known as "29A" and sent to anti-virus groups. Thus, it should be regarded as a potential (but not real) security threat to Bluetooth or Symbian OS since the virus has never spread outside of this system.

In August 2004, a world-record-setting experiment (see also Bluetooth sniping) showed that the range of Class 2 Bluetooth radios could be extended to 1.78 km (1.08 mile) with directional antennas and signal amplifiers.[29] This poses a potential security threat because it enables attackers to access vulnerable Bluetooth-devices from a distance beyond expectation. The attacker must also be able to receive information from the victim to set up a connection. No attack can be made against a Bluetooth device unless the attacker knows its Bluetooth address and which channels to transmit on.

2005

In January 2005, a mobile malware worm known as Lasco.A began targeting mobile phones using Symbian OS (Series 60 platform) using Bluetooth-enabled devices to replicate itself and spread to other devices. The worm is self-installing and begins once the mobile user approves the transfer of the file (velasco.sis) from another device. Once installed, the worm begins looking for other Bluetooth-enabled devices to infect. Additionally, the worm infects other .SIS files on the device, allowing replication to another device through use of removable media (Secure Digital, Compact Flash, etc.). The worm can render the mobile device unstable.[30]

In April 2005, Cambridge University security researchers published results of their actual implementation of passive attacks against the PIN-based pairing between commercial Bluetooth devices, confirming the attacks to be practicably fast and the Bluetooth symmetric key establishment method to be vulnerable. To rectify this vulnerability, they carried out an implementation which showed that stronger, asymmetric key establishment is feasible for certain classes of devices, such as mobile phones. [31]

In June 2005, Yaniv Shaked (http://www.eng.tau.ac.il/~shakedy) and Avishai Wool (http://www.eng.tau.ac.il/~yash/) published a paper describing both passive and active methods for obtaining the PIN for a Bluetooth link. The passive attack allows a suitably equipped attacker to eavesdrop on communications and spoof, if the attacker was present at the time of initial pairing. The active method makes use of a specially constructed message that must be inserted at a specific point in the protocol, to make the master and slave repeat the pairing process. After that, the first method can be used to crack the PIN. This attack's major weakness is that it requires the user of the devices under attack to re-enter the PIN during the attack when the device prompts them to. Also, this active attack probably requires custom hardware, since most commercially available Bluetooth devices are not capable of the timing necessary.[32]

In August 2005, police in Cambridgeshire, England, issued warnings about thieves using Bluetooth-enabled phones to track other devices left in cars. Police are advising users to ensure that any mobile networking connections are de-activated if laptops and other devices are left in this way.[33]

2006

In April 2006, researchers from Secure Network and F-Secure published a report that warns of the large number of devices left in a visible state, and issued statistics on the spread of various Bluetooth services and the ease of spread of an eventual Bluetooth worm.[34]

2007

In October 2007, at the Luxemburgish Hack.lu Security Conference, Kevin Finistere and Thierry Zoller demonstrated and released a remote root shell via Bluetooth on Mac OS X v10.3.9 and v10.4. They also demonstrated the first Bluetooth PIN and Linkkeys cracker, which is based on the research of Wool and Shaked.

Health concerns

Bluetooth uses the microwave radio frequency spectrum in the 2.4 GHz to 2.4835 GHz range. Maximum power output from a Bluetooth radio is 100 mW, 2.5 mW, and 1 mW for Class 1, Class 2, and Class 3 devices respectively, which puts Class 1 at roughly the same level as mobile phones, and the other two classes much lower.[35] Accordingly, Class 2 and Class 3 Bluetooth devices are considered less of a potential hazard than mobile phones, and Class 1 may be comparable to that of mobile phones.

See also

- Bluejacking
- Bluesniping
- Java APIs for Bluetooth
- Jellingspot Data Server
- Handsfree
- IEEE 802.15
- List of computer standards
- Near Field Communication
- Personal Area Network
- Tethering
- Wibree - complementary standard with lower power consumption, developed by Nokia, now named ULP Bluetooth.
- Wireless USB
- ZigBee - low power lightweight wireless protocol in the ISM band.

References

1. ^ Monson, Heidi (1999-12-14). "Bluetooth Technology and Implications". SysOpt.com. http://www.sysopt.com/features/network/article.php/3532506. Retrieved on 2009-02-17.
2. ^ "About the Bluetooth SIG". Bluetooth SIG. http://www.bluetooth.com/Bluetooth/SIG/. Retrieved on 2008-02-01.
3. ^ Kardach, Jim (2008-05-03). "How Bluetooth got its name". http://www.eetimes.eu/scandinavia/206902019?cid=RSSfeed_eetimesEU_scandinavia. Retrieved on 2009-02-24.
4. ^ [a] [b] Newton, Harold. (2007). *Newton's telecom dictionary.* New York: Flatiron Publishing.

5. ^ "How Bluetooth Technology Works". Bluetooth SIG. http://www.bluetooth.com/Bluetooth/Technology/Works/. Retrieved on 2008-02-01.
6. ^ "Wii Controller". Bluetooth SIG. http://bluetooth.com/Bluetooth/Products/Products/Product_Details.htm?ProductID=2951. Retrieved on 2008-02-01.
7. ^ Apple (2002-07-17). *Apple Introduces "Jaguar," the Next Major Release of Mac OS X*. Press release. http://www.apple.com/pr/library/2002/jul/17jaguar.html. Retrieved on 2008-02-04.
8. ^ "Network Protection Technologie". *Changes to Functionality in Microsoft Windows XP Service Pack 2*. Microsoft Technet. http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx. Retrieved on 2008-02-01.
9. ^ BlueZ - Official Linux Bluetooth protocol stack (http://www.bluez.org)
10. ^ "The Bluetooth Blues". Information Age. 2001-05-24. http://www.information-age.com/article/2001/may/the_bluetooth_blues. Retrieved on 2008-02-01.
11. ^ Guy Kewney (2004-11-16). "High speed Bluetooth comes a step closer: enhanced data rate approved". Newswireless.net. http://www.newswireless.net/index.cfm/article/629. Retrieved on 2008-02-04.
12. ^ [a] [b] [c] "Specification Documents". Bluetooth SIG. http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/. Retrieved on 2008-02-04.
13. ^ "HTC TyTN Specification" (PDF). HTC. http://www.europe.htc.com/z/pdf/products/1766_TyTN_LFLT_OUT.PDF. Retrieved on 2008-02-04.
14. ^ (PDF) *Simple Pairing Whitepaper*. Version V10r00. Bluetooth SIG. 2006-08-03. http://bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf. Retrieved on 2007-02-01.
15. ^ Michael Oryl (2007-03-15). "Bluetooth 2.1 Offers Touch Based Pairing, Reduced Power Consumption". MobileBurn. http://www.mobileburn.com/news.jsp?Id=3213. Retrieved on 2008-02-04.
16. ^ Taoufik Ghanname (2007-02-14). "How NFC can to speed Bluetooth transactions-today". Wireless Net DesignLine. http://www.wirelessnetdesignline.com/howto/showArticle.jhtml?articleID=180201430. Retrieved on 2008-02-04.
17. ^ David Meyer (2009-04-22). "Bluetooth 3.0 released without ultrawideband". zdnet.co.uk. http://news.zdnet.co.uk/communications/0,1000000085,39643174,00.htm. Retrieved on 2009-04-22.
18. ^ Nokia (2007-06-12) (PDF). *Wibree forum merges with Bluetooth SIG*. Press release. http://www.wibree.com/press/Wibree_pressrelease_final_1206.pdf. Retrieved on 2008-02-04.
19. ^ [1] (http://www.wimedia.org/) , [2] (http://www.wimedia.org/imwp/download.asp?ContentID=15508) , [3] (http://www.wimedia.org/imwp/download.asp?ContentID=15506) , [4] (http://www.bluetooth.com/Bluetooth/Technology/Technology_Transfer/) , [5] (http://www.usb.org/press/WiMedia_Tech_Transfer/) , [6] (http://www.incisor.tv/2009/03/what-to-make-of-bluetooth-sig-wimedia.html)
20. ^ [a] [b] Stallings, William. (2005). *Wireless communications & networks*. Upper Saddle River, NJ: Pearson Prentice Hall.
21. ^ Juha T. Vainio (2000-05-25). "Bluetooth Security". Helsinki University of Technology. http://www.iki.fi/jiitv/bluesec.pdf. Retrieved on 2009-01-01.
22. ^ Andreas Becker (2007-08-16) (PDF). *Bluetooth Security & Hacks*. Ruhr-Universität Bochum. http://gsyc.es/~anto/ubicuos2/bluetooth_security_and_hacks.pdf. Retrieved on 2007-10-10.
23. ^ Scarfone, K., and Padgette, J. (September 2008) (PDF). *Guide to Bluetooth Security*. National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf. Retrieved on 2008-10-03.
24. ^ "What is bluejacking?". Helsinki University of Technology. http://www.bluejackq.com/what-is-bluejacking.shtml. Retrieved on 2008-05-01.
25. ^ "Security Weaknesses in Bluetooth". RSA Security Conf. – Cryptographer's Track. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.23.7357. Retrieved on 2009-03-01.
26. ^ "Bluetooth". The Bunker. http://www.thebunker.net/resources/bluetooth. Retrieved on 2007-02-01.
27. ^ "BlueBug". Trifinite.org. http://trifinite.org/trifinite_stuff_bluebug.html. Retrieved on 2007-02-01.
28. ^ John Oates (2004-06-15). "Virus attacks mobiles via Bluetooth". The Register. http://www.theregister.co.uk/2004/06/15/symbian_virus/. Retrieved on 2007-02-01.
29. ^ "Long Distance Snarf". Trifinite.org. http://trifinite.org/trifinite_stuff_lds.html. Retrieved on 2007-02-01.
30. ^ "F-Secure Malware Information Pages: Lasco.A". F-Secure.com. http://www.f-secure.com/v-descs/lasco_a.shtml. Retrieved on 2008-05-05.

31. ^ Ford-Long Wong, Frank Stajano, Jolyon Clulow (2005-04) (PDF). *Repairing the Bluetooth pairing protocol.* University of Cambridge Computer Laboratory. http://www.cl.cam.ac.uk/~fw242/publications/2005-WongStaClu-bluetooth.pdf. Retrieved on 2007-02-01.
32. ^ Yaniv Shaked, Avishai Wool (2005-05-02). *Cracking the Bluetooth PIN.* School of Electrical Engineering Systems, Tel Aviv University. http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/. Retrieved on 2007-02-01.
33. ^ "Phone pirates in seek and steal mission". Cambridge Evening News. Archived from the original on 2007-07-17. http://web.archive.org/web/20070717035938/http://www.cambridge-news.co.uk/news/region_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf. Retrieved on 2008-02-04.
34. ^ (PDF) *Going Around with Bluetooth in Full Safety.* F-Secure. 2006-05. http://www.securenetwork.it/bluebag_brochure.pdf. Retrieved on 2008-02-04.
35. ^ M. Hietanen, T. Alanko (2005-10). "Occupational Exposure Related to Radiofrequency Fields from Wireless Communication Systems" (PDF). *XXVIIIth General Assembly of URSI - Proceedings.* Union Radio-Scientifique Internationale. http://www.ursi.org/Proceedings/ProcGA05/pdf/K03.7(01682).pdf. Retrieved on 2007-04-19.

External links

- Bluetooth Special Interest Group Site (includes specifications) (http://www.bluetooth.org)
- Official Bluetooth site aimed at users (http://www.bluetooth.com)
- Official Bluetooth gadget guide, aimed at users (http://gadgetguide.bluetooth.com)
- OMTP Bluetooth Local Connectivity Paper (http://www.omtp.org/Publications/Display.aspx?Id=8f152a02-4120-4933-a1e5-74c7ad472bc8)
- Bluetooth affect other 3G & IMT-2000 (aka WiMAX devices) (http://news.softpedia.com/news/Bluetooth-over-Wi-Fi-Kills-Nearby-WiMax-Networks-81415.shtml) , Softpedia Report

Internet access								
Network type	Wired					Wireless		
	Optical	Coaxial cable	Ethernet cable	Phone line	Power line	Unlicensed terrestrial bands	Licensed terrestrial bands	Satellite
LAN	1000BASE-X	G.hn	Ethernet	HomePNA · G.hn	G.hn	Wi-Fi · **Bluetooth** · DECT · Wireless USB		
WAN	PON	DOCSIS		Dial-up · ISDN · DSL	BPL	Muni Wi-Fi	GPRS · iBurst · WiBro/WiMAX · UMTS-TDD, HSPA · EVDO · LTE	Satellite